Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 15 (2011) 4574 – 4578

Procedia Engineering

www.elsevier.com/locate/procedia

Advanced in Control Engineering and Information Science

System Recovery Testing of Hardware Firewall

Liang Zhi-hong[a], Luo Jian-zhen[b], Liang Zhi-qiang[a] a*

[a]*Electric Power Research Institute of Guangdong Power Grid Corporation, Guangzhou, China*
[b]*School of Information Science and Technology, Sun Yat-Sen University, Guangzhou, China*

Abstract

System recovery is described to characterize the ability that a firewall under testing recovers from an overload condition. In our paper, we present an approach to test the system recovery base on the traffic whose frame size obeys a specific distribution and figure out the system recovery time and the variance of the system recovery time. We implement the testing base on stress condition with overload traffic in different duration to figure out the *D-d* curve, which helps to show the stability of the system recovery time as the duration of overload traffic increasing.

Keywords: system recovery; hardware firewall; stability

1. Introduction

Firewalls [1, 2], which are essentially a collection of active network elements, are a widely used to control the access to computers in an internal network and services implemented on them. Firewalls perform to filter undesired traffic out of the data flow travelling from or to a protected network. According to various firewall users, the security policy of the firewall varies from network to network, so firewalls can be configured to implement various security policies.

Firewalls have to be tested to validate whether they implement as specified or not. There are several approaches of testing firewall, such as implementation testing, performance testing and penetration testing. However, general testing approaches concern about the implementation and performance of

* Corresponding author. Tel.: +86-15915892125.
E-mail address: liangzhihong@gddky.csg.cn .

doi:10.1016/j.proeng.2011.08.859

firewall. In fact, network managers are also interested in the behaviors and the weakness of firewalls in an extreme environment. Moreover, the speed at which a firewall recovers from an overload condition is very important parameter to network managers. However, little work was done to the problems.

In this paper, we are aim to tackle with the problem mentioned above, we propose an approach to test the hardware firewall's System Recovery[3] base on the traffic whose frame size obeys a specific distribution. We implement our method to characterize the speed at which the firewall system recovers from overload condition and reveal the stability of the system recovery of the firewall system in different stress condition.

2. Related Works

There are several approaches to test firewalls [4, 5, 6]. Penetration testing [7] reveals security flaws of a firewall by running attacks against it. Firewall implementation testing is primarily performed by the firewall vendors to increase the reliability of their products. Testing of the firewall rules verifies weather the security policies are correctly implemented by a set of firewall rules. Performance analysis tests are conducted to evaluate the throughput and processing capacity of the firewall.

[8] shows how a network security policy can be formally specified in a high-level way. This approach tests conformance to a specified policy. In order to formally model the firewalls and the surrounding network and to mechanically derive test-cases checking the firewalls for vulnerabilities, [9] proposes a specification-based testing of firewalls to open up the possibility to go beyond test-sequence generation and performs the real testing automatically on a real system. [10] presents the necessity and the importance of a stress testing for hardware and software.

In this paper, we introduce an approach to test the system recovery time of the firewall. We conduct the firewall testing in the traffic whose frame size obeys a specific distribution to figure out the average value of system recovery time and the variance of the recovery time. Besides, we implement the testing base on stress condition with overload traffic in different duration to figure out the D-d curve, which helps network managers to study the trend of the system recovery time when the duration of overload traffic increases.

3. Methodology

In this section, we propose an approach to test the system recovery of firewalls. Our testing performs in traffic whose statistical distribution is the same with that in a real environment. We introduce the average of system recovery time to gauge the system recovery of firewalls and the variance of system recovery time to evaluate the stability of firewall's system recovery.

Using traditional method [3] of testing system recovery, one can only know about the system recovery based on traffic of one frame size. However, in real world, the frame size in traffic always has a statistical distribution. Average of the system recovery time does not indicate the stability of the recovery time. Actually, network managers also wonder whether the system is stable enough to recovery from an abnormal situation. Traditional method does not reveal the ability and stability under different duration of stress condition.

In order to tackle the problem mentioned above. We propose an approach to test the system recovery of firewall. In contrary to traditional approach, our approach involves the traffic who frame size obeys the statistical distribution of that in a real environment, and the trials will be repeated for several times (10 times, for example) to calculate the average and variance of the testing results.

In order to reflect the states in a real-world circumstance, we improve our scheme to involve the traffic whose frame size obeys the statistical distribution in real-world. First, we have to sample the traffic in the

firewall, and analyze the sample data from the firewall's network environment to figure out the sample distribution. Secondly, we send a data flow at a rate of 110% of system's throughput, to the firewall under testing for a period (we recommend 60 second at least). We reduce the traffic rate to 50% of the above rate at timestamp *A*. Then monitor the output to record the time(timestamp *B*) of the last frame loss by the system, finally, the recovery time, noted by t_j, should be figured out by abstract timestamp *A* from timestamp *B*, that is t_j = timestamp *B* – timestamp *A*.

Repeat these procedures for several times, record the system recovery time. Assume that we repeat the trials for *n* times, and the results are recorded as t_j, where $j = 1,2,3,\ldots,n$. Then we have the average of the system recovery time, noted by *T*, and the variance of the system recovery time, noted by *D*. A small system recovery time means a high speed the system recover from an overload circumstance. Small value of variance of the system recovery time is referred to as stable recovery ability.

In order to figure out the stability of system recovery of the firewall in different stress condition, we change the duration of the overload traffic, and we test the system recovery average time value of 10 times, and draw a *D-d* curve to show stability of the system recovery time vary with different duration of overload condition period.

First, we send a data flow at a rate of 110% of system's throughput, to the firewall under testing for a specific duration. The duration in the paper is chose as 5, 10, 30, 60, 120, 600 (All the value listed above measured in second) Second, at the timestamp *A*, we reduce the traffic, record the time (timestamp *B*) of the last frame loss by the firewall. The recovery time should be figured out by abstract timestamp *A* from timestamp *B*, that is timestamp *B* – timestamp *A*.

For each duration, repeat these procedures for several times, record the determined system recovery time. For each duration *d*, we have the average system recovery time T_d and the variance of system recovery D_d, (d = 5, 10, 30, 60, 300, 600).

The final work is drawing the curve according to the result. The horizontal axis lays the value of the duration, while the vertical axis lays the value of D_d corresponding to the duration value *d*, noted by the horizontal axis. We call this curve as *D-d* curve.

4. Case study

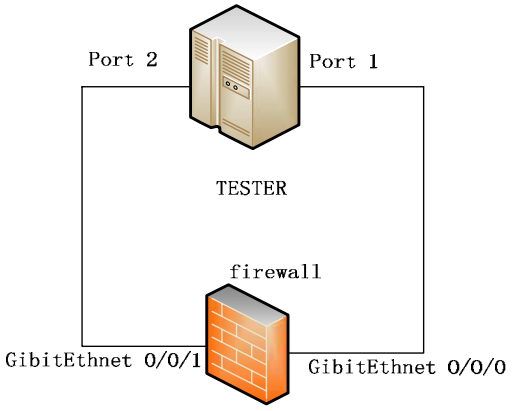

Fig. 1. Test bed for system recovery

In this case, we test the system recovery of a hardware firewall. The test bed is show as Fig. 1. We set the firewall as the transparent mode. The tester send flows from port 1 to the firewall, receive the data in port 2. The data flow is set to be unidirectional.

The statistical distribution of frame size of data set is listed as Table 1. Based on this data set, the throughput of the firewall is 1000fps.

Table 1. The statistical distribution of data set

IP total length	Default Ethernet	weight	percentage
72	90	5867	58.6%
74	92	200	2%
576	594	2366	23.66%
1500	1518	1567	15.6%

In the case study, we choose the duration of overload as 5 second, 10 second, 30 second, 60 second, 300 second, 600 second. For each duration, noted by *d*, we send a data flow in the rate of 110% of the firewall's throughput for a period of d, and reduce the data rate to 50 of the above rate at time *A*. Then, we find out the time *B* when the last frame dropped by the firewall. The system recovery is $t = B - A$. Repeat the procedure, and calculate the average and variance of system recovery *t*. The result of in this case is shown in Table 2. The variance is noted by *D*, and the average is noted by *T*.

Table 2. *D* and *T* of the system recovery

d	5	10	30	60	120	300	600
D	0.00012	0.00081	0.00004	0.00003	0.00011	0.00015	0.00005
T	1.0013	1.9604	1.966	1.9452	1.926	1.906	1.866

Based on the result shown in Table 2, the *D-d* curve in this case is shown in Fig. 2.

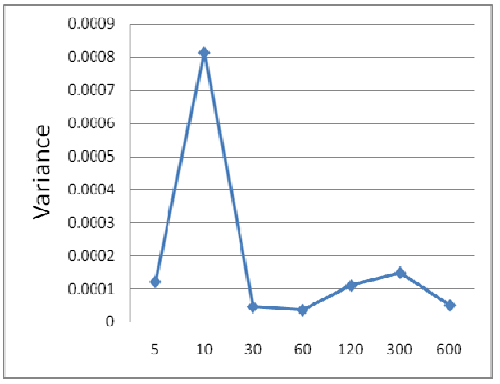

Fig. 2. D-d curve for the firewall

From Table 2 and Fig. 2, we can see that variances are less than 0.0009, which is so samll that we can regard it as zero. This indicates that, the system recovery is very stable. Moreover, the variance for

duration of 10 second is bigger than others. That means the system recovery for duration of 10 second is less stable than that of other durations.

5. Summary

In our paper, we present an approach to test the system recovery time of hardware firewall. Our contribution in this paper is that we build the firewall testing involving the traffic whose frame size obey a specific statistical distribution to reveal the ability of firewall to recover from an overload condition and the variance of the ability. Moreover, we implement the testing base on stress condition with overload traffic in different duration to draw the *D-d* curve, which helps to indicate the trend of the stability of system recovery when the duration of overload traffic increases.

Acknowledgements

We would also like to thank Bochao Lee and the anonymous reviewers for their help to improve this paper.

References

[1] W. Cheswick, 1990. The design of a secure Internet gateway. In: USENIX, Anaheim, CA, USA, June 1990, pp. 233 – 237.

[2] S.Ioannidis , A.D. Keromytis , S.M. Bellovin , J.M. Smith, Implementing a distributed firewall, Proceedings of the 7th ACM conference on Computer and communications security, pp. 190-199, November 01-04, 2000,

[3] S. Bradner, J. McQuaid, RFC 2544: Benchmarking Methodology for Network Interconnection Devices, http://datatracker.ietf.org/doc/rfc2544/

[4] E. Schultz, 1996. How to perform effective firewall testing. Computer Security Journal, Vol. 12, No. 1, 1996, pp. 47 – 54.

[5] E. Schultz, 1997. When firewalls fail: lessons learned from firewall testing. Network Security, February 1997, pp. 8-11.

[6] M.R. Lyu and L.K.Y. Lau, 2000. Firewall security: policies, testing and performance evaluation. Proceedings of the COMSAC. IEEE Computer Society, 2000, pp. 116-21.

[7] B. Arkin, S. Stender, G. McGraw, Software Penetration Testing, IEEE Security and Privacy, v.3 n.1, pp.84-87, January 2005

[8] D. Senn, D. A. Basin, and G. Caronni. Firewall conformance testing. Testing of Communicating Systems, pp. 226-241, 2005

[9] J. Jürjens, and G. Wimmel. Specification-based testing of firewalls. In Andrei Ershov, editor, 4th International Conference Perspectives of System Informatics (PSI'01), LNCS. Springer, 2001

[10] H. A. Chan, Accelerated stress testing for both hardware and software. International symposium on product quality and integrity, Los Angeles CA, 2004, pp. 346-351